MULTIMEDIA UNIVERSITY®

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2017/2018

ETM7106 – NETWORK SECURITY

15 MARCH 2018
7.30pm - 10.30pm
(3 Hours)

INSTRUCTIONS TO STUDENT

1. This examination paper consists of 6 pages including the cover page with 4 questions only.
2. Attempt **ALL** questions. All questions carry equal marks and the distribution of the marks for each question is given.
3. Please print all your answers in the Answer Booklet provided.

Question 1

a) Consider the AES-128 block cipher. What **effort** is required for an *exhaustive key search*? If it is claimed that a *shortcut attack* exists on AES-128, discuss what is the maximal amount of computational effort that it should have in order to be considered as a meaningful shortcut attack.

[2+2 marks]

b) Describe what you understand by a *hash function* in terms of its inputs and outputs, and what **properties** are expected or commonly observed about its inputs and outputs. [3+2 marks]

c) Given a digital *signature scheme* $Sig(x,y)$ acting on some inputs x and y to produce some output z, and a *hash function* $h(w)$ acting on an input w to produce an output x. With appropriate notations of your choice, show how **digital signing** is performed including how a hash function is used in relation to a signature.

[3 marks]

d) Consider the Mini-AES' *MixColumns* operation, wherein multiplication of two nibbles are to be performed modulo $m(x) = x^4+x+1$. Show how the **multiplication** of 0010 and 1110 is done modulo $m(x)$. [8 marks]

Question 2

a) Describe THREE **types** of *Authentication factors* and explain how these are used for for the problem of *access control*. [2+2+2 marks]

b) Consider an adversary against a *digital signature scheme* being used in online transactions. Discuss **how** an adversary could **interact** with the scheme, and then discuss **what goal(s)** that the adversary would want to achieve against this scheme. [3+3 marks]

Continued...

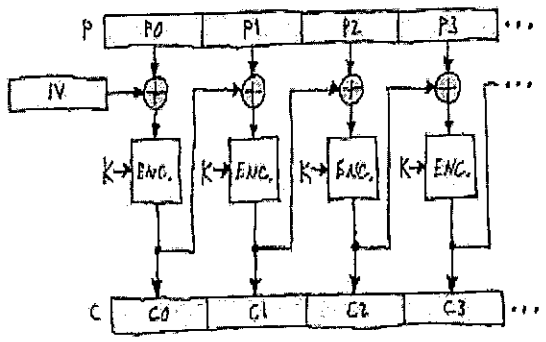

Figure 1 [sourced from www.cs.rit.edu/~ark]

c) Figure 1 shows a way in which a *block cipher E* can be used in commercial systems such as SSL/TLS and IPsec.

(i) Discuss if the *security property* of **confidentiality** can be achieved when a block cipher is used in this way. [2+3 marks]

(ii) The *initialization vector* IV is known, while the output ciphertext blocks C0, …, C3 are sent to the recipient. If block C2 is received in **error**, which plaintext blocks would be recovered in error? [3 marks]

Question 3

a) Describe your understanding of the **discrete logarithm problem** and how it is related to security. [3 marks]

b) The *RSA public key cipher* performs encryption defined as follows

$$c = m^e \bmod n$$

where c is the ciphertext, m the plaintext, e the public key and n the modulus, and decryption is defined as

$$m = c^d \bmod n.$$

Given that the public key e is 37, private key d is 13, and modulus n is 40; show how a plaintext $m = 3$ can be **encrypted**. [9 marks]

Continued…

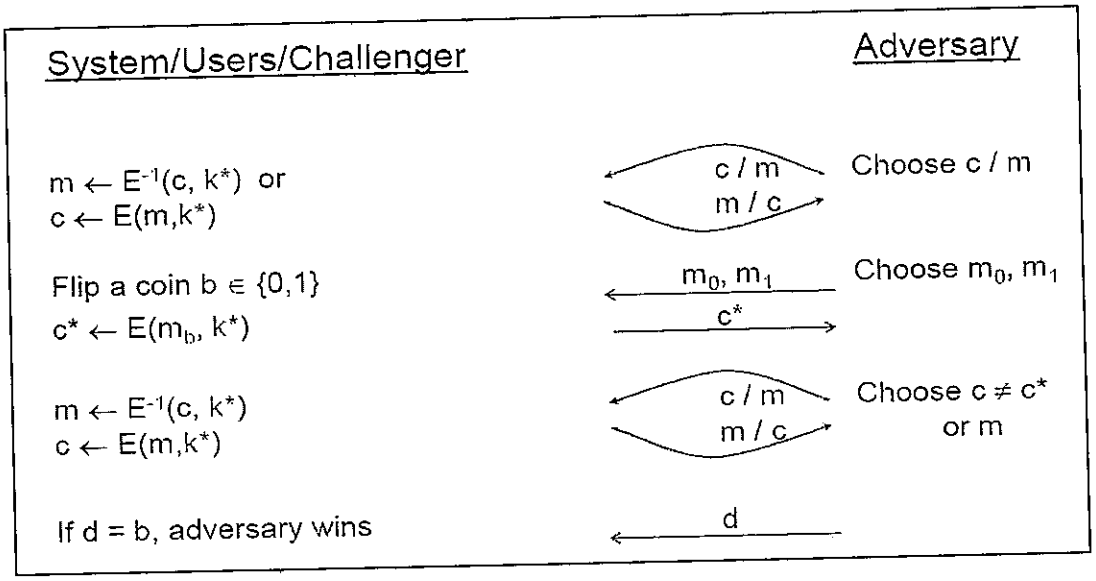

Figure 2

c) Figure 2 shows the the *indistinguishability against chosen-ciphertext attacks* (IND-CCA) adversarial model; this type of model is required for proving the security of public-key ciphers, which are now commonly found in various security standards like IEEE P1363, ISO/IEC 18033, IEEE 802.11-2012, IEEE 1619 and Bluetooth.

(i) Describe how this security model relates to the **security** of *e-voting*. [4 marks]

(ii) Based on your understanding, is the encryption considered in Figure 2 of the type **symmetric encryption** or **public key encryption**? Explain. [4 marks]

Continued...

Question 4

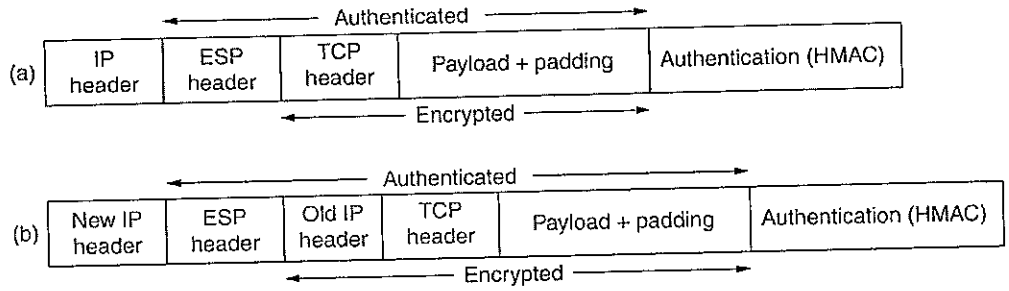

Figure 3

a) Figure 3 illustrates the ESP (encapsulating security payload) mechanism of IPsec for securing the IP layer. In particular, Figure 3(a) is for ESP transport mode and Figure 3(b) for ESP tunnel mode.

i) Describe the main differences between the two modes. [3 marks]

ii) Discuss why encryption and authentication are applied to different fields not in common? [2+2 marks]

b) Describe the basic concept behind how *intrusion resilience* is performed, compared to *intrusion detection* or *intrusion prevention*. [3 marks]

Continued...

c) Describe various **approaches** used by attackers to design *malware* into mobile phone Apps. [4 marks]

d) Describe your understanding of the following compromise resilience strategies using some examples of how they are provided in real networked systems:

(i) Perfect forward secrecy

[3 marks]

(ii) Leakage resilience

[3 marks]

End of Paper